REMARKS/ARGUMENTS

Claim Amendments

The Applicant has amended claims 1, 6, 7, 9-11, and 15-18. Applicant respectfully submits no new matter has been added. Accordingly, claims 1-19 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

Claim Rejections – 35 U.S.C. § 112

Claims 1-19 stand rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter as the invention. In paragraph 2 of the Detailed Action, the examiner indicated that "a global Single-Sign-On Front End (G_SS)-FE) infrastructure" was not described.

The Applicant respectfully disagrees. In paragraph [0080] the GG-SSO-FE is discussed ; "[T]hus, the Service Provider (2) does not need to be aware of the user's National Network Operators (N-MNO-A), but just contact a site where the authentication assertion was generated and check that such site is trusted. In short, this entry point (33) in the federation, namely a Global SSO Front End (G-SSO-FE) infrastructure, ...". The entry point in the federation of networks is the G-SSO-FE.

The term Federation is defined in paragraph [0007]: "This way allows an SP and an (identity provider) to provide a user with SSO facilities when accessing to different services in the Internet. The SP and the IdP are assumed to have signed a bilateral agreement in advance, thus forming a so-called Federation." (emphasis added)

Further, in paragraph [0001] "The present invention generally relates to Single Sign-On services for a plurality of users accessing a service network via Internet through a packet radio network. More particularly, the invention relates to a telecommunication system and a method for providing Single Sign-On services to users of a Service Network owned by a multinational network operator through a packet radio network where the users are roaming." The Applicant respectfully submits that one skilled in the art of telecommunication via Internet through a packet radio network would be enabled to make or use the invention as described in the Specification.

Also, in paragraph [0079] of the Specification, "[I]n this respect, this single logical entry point (33) for a Single Sign-On (SSO) service does not imply a single physical entry point, but rather each individual Service Provider (2) may actually have a different URI where the user's browser, or more generally speaking a user's agent, is redirected. Thus, a single entry point implies that a SSO service, which is intended for deciding whether or not a user is trusted, is globally used within the network owned or controlled by the Multinational Mobile Network Operator (1) and, thereby, a given Service Provider can change the physical SSO entry point (33) towards the federation while keeping the same functionality toward the user.

In paragraph 3 of the Detailed action Claims 1, 2, 6, 7, 10 and 18 are rejected as indefinite. The term Multinational Network Operators was stated as being unclear. The Applicant respectfully refers to the specification in paragraph [0003]: "the MNO is a network operator that likely has acquired smaller operators in different countries and indicates the larger wireless network operators such as Orange, AT&T, Verizon, TMobile, etc." Furthermore, the preamble to the independent claims clearly states "...[a] packet radio network of a Multinational Mobile Network Operator..." which refers to networks of the MMNOs. In the dependent claims, the items such as "service agreements with the Multinational Mobile Network Operator" do not refer to wireless connections, but to agreements between operators.

The Applicant appreciates the thorough review of the Specification and has corrected the unclear statements in claims 1 and 10. Support for the changes is found in paragraph [0055]. The scope of global Single-Sign-On Front End is discussed above.

The Applicants have corrected the deficiencies and the Applicants respectfully submit the subject claims are now allowable.

Claim Rejections – 35 U.S.C. § 103 (a)

Claims 1-14 and 19 stand rejected under 35 U.S.C. § 103(a) as obvious over WO 02/011467 to Jones et al (hereinafter "Jones") in view of U.S. Pat. Pub. No. 2003/0051041 to Kalavade et al. (hereinafter "Kalavade"). The Applicant respectfully traverses the rejection of these claims.

As amended claim 1 discloses that when a user attempts to sign on to one of the service providers in a federation of MNOs, the SP provides a specific URI as a Single Sign-On entry point towards the federation. The provided SSO point is trusted by the rest of the MNOs in the federation. As the user roams through the federation each Service Provider that receives a sign on request from the user receives a token where the authentication assertion of the user was generated (specific URI). The SP checks that the site is trusted and if so, the user is logged into the SP. In other words, the user can sign on to one of any number of "trusted" sites and any subsequent SP receives notification that the user is authenticated at a trusted site, which is part of the Global Single Sign-On Front End. (para. 79-82)

The Jones reference is cited for disclosing Single Sign-On utilizing a home RADIUS server and broadly interprets Jones configuration as comparable to the G-SSO-FE of the Applicant's present application. "Each wireless access user has a personal computer PC and a UMTS user equipment (UE) 21'and 22'with a directly attached antenna 20 and is connected by typical data connections such as an RS232, USB or Ethernet to the PC." (second paragraph of Detailed Description). However, the user equipment in the Jones reference requires being connected through the Internet by the user's PC to the RADIUS server. The Kalavade reference is cited for teaching a converged billing/authentication gateway that maintains billing records for a roaming user. Kalavade is cited for modifying the visited AAA server of Jones to include the capability of binding a user's identifiers with the home AAA server.

SSO applies to one user accessing a first network where the user is authenticated and then to a second network which trusts the authentication of the first network. The Applicant respectfully submits that neither Jones nor Kalavade, individually or in combination, disclose authentication for a federation of MNOs through the use of multiple entry points in multiple connected networks in the federation. This being the case, the applicant respectfully requests the allowance of independent claims 1 and 10 and the respective dependent claims 2-9, 11-14 and19.

Claims 15-18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Jones and Kalavade as applied to claims 1-14 above, and further in view of U.S. Patent 6,578,085 to Khalil et al (hereinafter "Khalil"). The Applicant respectfully traverses the rejection of these claims.

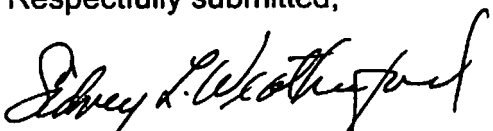
The Khalil reference is cited for disclosing tracking IP addresses for rejecting the element s determining the visited network which assigned the current IP address to the user". The Applicant respectfully submits that Khalil does not disclose the elements missing from the Jones and Kalvade references as noted above. Therefore, the Applicant respectfully requests the allowance of claims 15-18 as these claims depend from amended claim 10 and recited further limitations.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,



By Sidney L. Weatherford
Registration No. 45,602

Date: May 4, 2009

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-8656
sidney.weatherford@ericsson.com